

REMARKS

This paper is responsive to an Office Action mailed July 30, 2007. Prior to this response, claims 1-34 were pending. After amending claims 1-5, 13-20, 27, 30-31, and 34, and canceling claims 11-12, 28-29, and 32-33, claims 1-10, 13-27, 30-31, and 34 remain pending.

In Section 3 of the Office Action claims 1 through 34 have been rejected under 35 U.S.C. 103(a) as unpatentable with respect to Morgan et al. ("Morgan"; US 5,220,674) in view of Wiegley (US 6, 711, 677) and Konsella et al. (US 6,856,317). With respect to claim 1, the Office Action acknowledges that Morgan fails to disclose receiving CK, an asymmetrical encrypted key (K) encrypted using an asymmetrical encryption public key (pubK). The Office Action also states that Morgan fails to disclose receiving CH, a hash of the job encrypted using K, decrypting CK using an asymmetrical encryption private key privK to recover K, hashing the job, generating H', and using K to validate CH. The Office Action states that Wiegley discloses these features and it would've been obvious to add the security features taught by Wiegley to Morgan. The Office Action states that the motivation for combining the references would be to provide security to the access and use of network-connected resources by validating the print job. The Office Action states that Konsella discloses a method for storing secure data in a font file, which is a form of printing resource. The Office Action states that it would've been obvious to add the cryptographic security taught by Konsella in to the network-connected resources of Morgan because secure font files can be easily stored in a printer server. The motivation for

combining would be to provide security using network-connected resources such as fonts and for ease of maintaining the secured resources. This rejection is traversed as follows.

An invention is unpatentable if the differences between it and the prior art would have been obvious at the time of the invention. As stated in MPEP § 2143, there are three requirements to establish a *prima facie* case of obviousness.

First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck* 947 F.2d 488, 20 USPQ2d, 1438 (Fed. Cir. 1991).

Independent claims 1, 17-18, and 34 have been amended to recite that an unencrypted print job is sent along with CH_i and CK_i, responsive to key K_i, where each value of *i* is associated with a unique printer resource. That is, the claims limit a user to a particular resource corresponding to a particular key.

In column 6, lines 55 through 58, Morgan discloses a local area print server 10 which accepts print requests from printing clients 18 and arranges them to be serviced by printers 16. At column 7, lines 24 through 29, Morgan states that the local area print server may provide resources from an internal collection of resources, such as resource server 26, if printers 16 do not have a specific requested resource.

Wiegley discloses a print session occurring between a computer 12 and a printer 10. A secure print job is initially requested by computer 12 (Step 102). In response to receiving the request from the computer, the printer 10 generates a session identifier 38a (Step 104), which is stored in memory (col. 3, ln. 66 through col. 4, ln. 7). Next, the printer sends the session identifier and a public key to the computer (Step 106). The computer uses the public key to authenticate the printer (col. 4, ln. 30-42), Step 108. After the printer transmission is verified, the computer generates a secret encryption (session) key (Step 110). Using the printer's public key, the computer encrypts the session key and the session identifier (Steps 112 and 114). The print job is encrypted by the computer using the session key and sent to the printer (Steps 116 and 118). In Step 120, the printer decrypts the received session key using its private key. In Step 122 the printer compares the original session key to the decrypted session key, and if the keys match, the print job is processed in Step 126 (col. 4, ln. 47 through col. 5, ln 15).

For added security, the computer may generate a hash of the print job and encrypt it with the session key. The printer computes a hash value for the decrypted print job, and compares the computed hash value to the hash value received from the computer (col. 5, ln. 25-39).

Generally, Wiegley discloses a two-way communication process where link security is established in response to sending a session identifier to the node originating the print job, receiving a session identifier back in a reply, and comparing the received session identifier with the originally-sent identifier. In contrast, the claimed invention uses a one-way link between nodes – the claimed invention first device does not send a session identifier. Another general difference is that Wiegley's

process is designed to protect a print job being transmitted from one node to another. The claimed invention is designed to securely access a resource that is already stored in the memory of the destination node. Further, Wiegley does not disclose the processing of the print job using the decrypted resource.

Konsella discloses a process for storing public font data together with encrypted (secure) font data in a file (col. 2, ln. 54-63). At column 4, lines 44-56, Konsella discloses a security logic module 22 to manage secure font rasterization. A decryption key 28 or password can be provided to the font rasterizer by a user, to enable the font rasterizer to render secure glyphs based on entering the correct decryption key. However, Konsella does not disclose a secure means of transmitting or delivering a decryption key to a printer. Konsella does not disclose a means of associating encryption keys with particular secured resources.

The obviousness rejection appears to be based upon the assumption that the combination of the Morgan, Wiegley, and Konsella discloses all the limitations of the base claims. The base claims have been amended to recite that an unencrypted print job can be sent along with an encrypted hash (CH_i) and encrypted encryption key (CK_i), to access one resource from a plurality of encrypted resources. Alternately stated, each printer resource is associated with a particular key (K), so that a print job can be sent with information to unlock just one specific printer resource. Advantageously, this method permits printer resources to be allocated on the basis of a particular print job or a particular user. In contrast, the combination of references fails to disclose a secure means of delivering a combination of encrypted hash and encrypted encryption key that limits

access to just one particular resource, for one particular print job. With respect to the third *prima facie* requirement, even if Wiegley's encrypted transmission process is combined with Morgan's local area print server and Konsella's secure fonts, the combination still does not disclose the limitations of delivering a combination of encrypted hash and encrypted encryption key that limits access to just one particular resource, for one particular job. Therefore, the combination of references does not teach every limitation associated with claims 1, 17, 18, and 34. Claims 2-10 and 13-16, dependent from claim 1, claims 19-27 and 30-31, dependent from claim 18, enjoy the same distinctions.

With respect to the first *prima facie* requirement, the Office Action states that it would have been obvious to add the security features taught by Wiegley and Konsella to Morgan, with the motivation being to provide security to the access and use of network-connected resources by validating the print job. However, as noted above, none of the references disclose the transmission of a combination of encrypted hash and encrypted encryption key that limits access to just one particular resource. Further, the assumption of obviousness does not explain how a practitioner in the art could have modified Morgan to describe the claimed invention. It is not relevant if there is a suggestion to combine the prior art references if the combination fails to teach or suggest all the claimed invention limitations.

As noted in MPEP 2142:

The legal concept of *prima facie* obviousness is a procedural tool of examination which applies broadly to all

arts. It allocates who has the burden of going forward with production of evidence in each step of the examination process. See *In re Rinehart*, 531 F.2d 1048, 189 USPQ 143 (CCPA 1976); *In re Linter*, 458 F.2d 1013, 173 USPQ 560 (CCPA 1972); *In re Saunders*, 444 F.2d 599, 170 USPQ 213 (CCPA 1971); *In re Tiffin*, 443 F.2d 394, 170 USPQ 88 (CCPA 1971), *amended*, 448 F.2d 791, 171 USPQ 294 (CCPA 1971); *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967), *cert. denied*, 389 U.S. 1057 (1968). The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

A *prima facie* analysis is especially critical in the present circumstances since the rejection is predicated on limitations that are not explicitly disclosed in the prior art references. As noted in addressing the third *prima facie* requirement, even when combined, Morgan, Wiegley, and Konsella fail to disclose the delivery of a combination of an encrypted hash and encrypted encryption key that limits access to just one particular resource. More particularly, the Wiegley and Konsella references must suggest to an artisan that Morgan be modified to limit access to just one particular resource. The Applicant respectfully submits that it is not apparent that either Wiegley or Konsella can be used to suggest the Applicant's explicit encryption mechanism.

To support a *prima facie* case of obviousness based upon the modification of Morgan in light of Wiegley and Konsella, the Office Action must show the logic or thought process that an artisan might employ to change Morgan's process into one that incorporates all the Applicant's limitations. The Applicant respectfully submits that there is no language in the Wiegley and Konsella references that provides guidance for such modifications.

As another alternative, the *prima facie* case of obviousness based upon the modification of Morgan may be supported using the knowledge of a person with skill in the art, to supply the motivation lacking in the Morgan, Wiegley, and Konsella references. However, in this case it would be especially critical to supply evidence of the kind of knowledge that an artisan is assumed to have. Notable, when the source or motivation is not from the prior art references, "the evidence" of motive will likely consist of an explanation or a well-known principle or problem-solving strategy to be applied". *DyStar*, 464 F.3d at 1366, 80 USPQ2d at 1649. The Office Action has not supplied any explanation of how an artisan could possibly modify any of the references to yield all the explicit limitations recited in the base claim.

Considered from the perspective of the second *prima facie* requirement, the Office Action provides no evidence that the combination of teachings can be met with a reasonable expectation of success. The Applicant submits that a reasonable expectation cannot be found in the cited prior art references because the combination does not explicitly disclose or suggest all the limitations found in the Applicant's base claims.

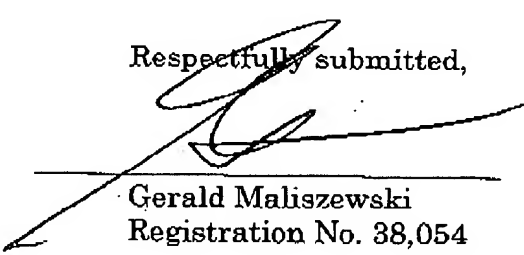
In summary, the Applicant respectfully submits that a *prima facie* case of obviousness has not been supported in the rejection of claims 1-10, 13-27, 30-31, and 34, and the Applicant respectfully requests that the rejection be removed.

It is believed that the application is in condition for allowance and reconsideration is earnestly solicited.

Date:

9/27/2007

Respectfully submitted,


Gerald Maliszewski
Registration No. 38,054

Customer Number 55,286
P.O. Box 270829
San Diego, CA 92198-2829
Telephone: (858) 451-9950
Facsimile: (858) 451-9869
gerry@ipatentit.net